UN Chief on launching the Advisory Body on

UN Chief on launching the Advisory Body on Artificial Intelligence (26 Oct 2023)

https://youtu.be/JbAVkD_DwgE?si=byaEsjS0sWm_eNGQ

LIVE: UN approves its first resolution on AI

https://www.youtube.com/live/aRZvrJ0asuc?si=FwfSa9sb9PuEMTRu

Shaping Responsible AI Governance: UN Chief' Address at AI for Global Good

https://youtu.be/82QQCHBVTws?si=sDK62rmwBqMOw5Rh

UN General Assembly passes resolution to govern artificial intelligence

https://youtu.be/YwO701_MxJ0?si=fQ5UNniqyk13WRZz

UN Chief on Digital Platforms policy brief - Press Conference (12 June 2023)

https://youtu.be/ktFF2dSH3oU?si=ZmieUbmAOtULuLxS

https://youtu.be/ktFF2dSH3oU?si=1x6L0SJnpl3l0sL_

General Assembly adopts landmark resolution on artificial intelligence

https://news.un.org/en/story/2024/03/1147831

UN General Assembly passes resolution to govern artificial intelligence

https://youtu.be/YwO701_MxJ0?si=OdWctPF2e95dt0mY

Artificial Intelligence: Press Conference | United Nations

https://youtu.be/jywAmR5pJ3Q?si=onmgHx5WDh20YFDq

UN News on X: "The UN General Assembly on Thursday adopted a landmark resolution on the promotion of “safe, secure and trustworthy” artificial intelligence (AI) systems that will also benefit sustainable development for all Read more

https://twitter.com/UN_News_Centre/status/1770897918947631197

https://twitter.com/UN_News_Centre/status/1770848178398466236

UN Chief on Digital Platforms policy brief - Press Conference (12 June)

https://youtu.be/ktFF2dSH3oU?si=ZmieUbmAOtULuLxS

Will the world get to grips with AI in 2024? | United Nations News

https://youtu.be/UNHhlZ3xOXs?si=nSxnRELuElYQHwEe

Consensus Adoption of U.S.-Led Resolution on Artificial Intelligence by the United Nations General Assembly
PRESS STATEMENT

ANTONY J. BLINKEN, SECRETARY OF STATE

MARCH 21, 2024

With today’s adoption in the UN General Assembly of the U.S.-led resolution on Artificial Intelligence (AI), UN Member States have spoken with one voice to define a global consensus on safe, secure, and trustworthy AI systems for advancing sustainable development. This consensus resolution, developed with direct input from more than 120 countries and cosponsored by more than 120 Member States from every region, is a landmark effort and a first-of-its-kind global approach to the development and use of this powerful emerging technology.

Artificial intelligence has enormous potential to advance sustainable development and the Sustainable Development Goals (SDGs). This resolution helps ensure that the benefits of AI reach countries from all regions and at all levels of development and

focuses on capacity building and bridging digital divides, especially for developing countries. It underscores the consensus that AI systems can respect human rights and fundamental freedoms, while delivering on aspirations for sustainable development, as these are fundamentally compatible goals.

Governments must work with the private sector, civil society, international and regional organizations, academia and research institutions and technical communities, and all other stakeholders to build this approach. Importantly, this resolution will serve as a foundation for multilateral AI efforts and existing and future UN initiatives.

The United States will continue to work with governments and other partners to ensure the design, development, deployment, and use of emerging technologies, including AI, are safe, secure, and trustworthy and are directed to achieving our common goals and solving our most pressing challenges.

https://www.state.gov/consensus-adoption-of-u-s-led-resolution-on-artificial-intelligence-by-the-united-nations-general-assembly/

Artificial Intelligence - Security Council: Communications Chief's Opening Remarks

https://youtu.be/5Z_nm5CRzlg?si=zYZKhl1QiciGi1hL

Generated by Google Gemini - UN General Assembly Resolution on AI

UN General Assembly resolution on Artificial Intelligence (AI) with relevant links:
Resolution Title: "Enhancing cooperation in the field of artificial intelligence in the context of sustainable development and the achievement of the Sustainable Development Goals"
Adopted by: The United Nations General Assembly on March 11, 2024
Key Points:
This is the first-ever UN resolution on AI, reflecting the growing global importance of the technology.
The resolution emphasizes the need for international cooperation to ensure AI is developed and used responsibly, ethically, and in a way that benefits all countries.
It highlights the potential of AI to contribute to achieving the UN's Sustainable Development Goals (SDGs) in areas like healthcare, education, and climate change.
Focus Areas:
Human rights and ethical considerations: The resolution calls on member states to develop and implement national frameworks for AI that respect human rights, including privacy, non-discrimination, and accountability.
Safety and security: It emphasizes the importance of ensuring AI systems are safe, secure, and trustworthy.
Transparency and explainability: The resolution encourages member states to promote transparency and explainability in AI systems, particularly in decision-making processes.
Inclusiveness and accessibility: It highlights the need for ensuring access to AI for all countries and promoting the development of AI that is inclusive and addresses the needs of all people.
Benefits of the Resolution:
Provides a framework for international cooperation on AI development and use.
Encourages responsible and ethical development of AI that respects human rights.
Promotes the potential of AI to contribute to solving global challenges.
Links:
Full Text of the Resolution: While the official UN website might take some time to update with the full text of the 2024 resolution, you can find the previous resolution (A/RES/76/168) that lays the groundwork for the 2024 update: https://quizlet.com/787069320/exam-2-international-relations-pt1-flash-cards/
UN News Article: This article provides a good overview of the resolution's key points: https://apnews.com/article/united-nations-artificial-intelligence-safety-resolution-vote-8079fe83111cced0f0717fdecefffb4d
AP News Article: This article offers a different perspective on the resolution, highlighting the collaboration between the US and China: https://apnews.com/article/united-nations-artificial-intelligence-safety-resolution-vote-8079fe83111cced0f0717fdecefffb4d
The UN General Assembly resolution on AI is a significant step forward in shaping the responsible development and use of this powerful technology. It sets the stage for continued international discussions and collaboration on AI governance to ensure its benefits reach everyone.

BBC.com: Neuralink video shows patient playing chess using brain implant

https://www.bbc.com/news/av/technology-68623380

Good Morning America: Neuralink claims 1st brain-chip patient can play chess

https://www.youtube.com/watch?v=cVo1G_Azte0

William and Mary AI and Cybersecurity

https://www.youtube.com/live/FKxzWl33Mko?si=S-NtQkMa7mcI4eGt

https://youtube.com/@wgcwm?si=gUloVidxKqd1zyje

https://youtube.com/@wgcwm?si=2BZBCRUDdoClP2UP

https://www.wm.edu/offices/wholeofgovernment/

William & Mary Libraries

https://youtu.be/07ilbLqlCuo?si=iFFubPAL1ZcaTyJF

WATCH: Jensen Huang's Nvidia GTC Keynote - LIVE

https://www.youtube.com/live/USlE2huSI_w?si=RRefAWkpMSft8ioY

The potential of AI-driven business solutions on the SME industry

https://www.youtube.com/live/gHRNv09TyP0?si=g6Ffi9iiN4iSXUZP

Cyber AGI Science DOC

https://drive.google.com/file/d/1YyBovajlUfnPhqyk03pTJtUAx-GcOPWM/view?usp=drivesdk

CyberAI Resource Document

https://drive.google.com/file/d/1NNhkOp0E627g7O0SMzrzOriT6ur87ZYA/view?usp=drivesdk

Cyber AI and AGI (Projection)

https://drive.google.com/file/d/1WczMfggo7XI1zSPC1T1XPPZ2ndpjv8-D/view?usp=drivesdk

Cyber AI Research and Analysis Document

https://drive.google.com/file/d/1NLTaaoNmALzkKS-dp7Pzkt7cqSYEC0qK/view?usp=drivesdk

Cybersecurity , Advanced Cyber Threat Intelligence and Artificial Intelligence Rationale and Paradigms .
Some Notes , Mind Maps , Infographics, Observations, Research and Analysis , CyberAI Blog Archives and web links , Updates on Relevant Seminars and Webinars , Assessments , Projections and Recommendations by Experts , Rendezvous on Cyber and AI with Perplexity AI , OpenAI's ChatGpt and Gemini Powered Google Bard AI .
Do it yourself guides , Instructubles . Learning Resources and Archives for Generative AI , Distributed Advanced Cyber Threat Intelligence, Open Source Software and OS Security , Quantum computing and Decentralised Mesh Computing , Concepts and Paradigms for Infosec , Indepth Countermeasures against Dis/Mis information and deepfakes , Free and Open Source Alternatives for CyberAI Services and Products, State of art evolving Concepts and Strategies – Beginner to Advanced .

DIY’s Instructubles and Self Help Guides . Learning Resources Archives for Generative AI , Distributed Advanced Cyber Threat Intelligence, Open Source Software and OS Security , Quantum and Decentralised Mesh Computing , Concepts and Paradigms for Infosec , Indepth Countermeasures against Dis/Mis information and deepfakes , FOSS Alternatives for CyberAI Services and Products, Cybersecurity Paradigms and State of art evolving Concepts and Strategies – Beginner to Advanced .
Global Standards for the above with respect to UN , US , EU , NATO , INDIA , GCC and relevant Cyber Defense and Intelligence Agencies and International Corporations . Readers Discretion is advised while assessing / analysing generative AI Content in the document .
DIYs KnowHow Instructables . Build Conceptual Clarity and Comprehend Global Perspectives on AI , Cyber defence and Advanced Cyber Intelligence – YouTube Playlists

Cyber Intelligence plus CyberSecurity and Countermeasures - DIY's , Guides , Instructables for OSS and OS Security , Application Security , Cyber threat Intelligence paradigms and Protocols etc by the supernatural forces and multilateral organisations of the Brilliant... perfectly beezer Human Race...298 Videos..

https://youtube.com/playlist?list=PLAOUl2tBZpjR2u2PaRnd6sE0EJSneu_4v&si=OV1CBLlzfqdfDIrk

167 video playlist for everything CyberAI for the foreseeable Complex yet intriguing future..Again by trenchant , effectual..smart as a whip..yet never predictable aces of everything CAI..in tactile flesh and blood..Enjoy Binge watching Cyber Defence Threat Intelligence with flavour of your acushla AI tardily but assuredly evolving..progressing towards AGI - Striking metamorphosis indeed..

https://youtube.com/playlist?list=PLAOUl2tBZpjS66nVEsFNozW8hfku73xSZ&si=awtGHMElEx8NdUS7

Cyber Threat Intelligence Playlist...195 videos...marking the geezerhood of association with the stonking anthropomorphic and sometimes fallible characteristics of your intelligent and precocious species that populated and reached 8.1 billion from 7 Billion on this one of a kind planet earth after the defuctness of terrestrials from Mesozoic era.

https://youtube.com/playlist?list=PLf-aX7Sa0eCRYUADIqTAU2qH-lKcNB-wj&si=L7N71nEaOquGe0eh

Autonomous Weapons Systems and Platforms - AWS UAVs UGVs

https://youtube.com/playlist?list=PLAOUl2tBZpjRCYH8AmTUwNt1z4hTH08QX&si=aWzgX2rq2Zg82ByU

CYber AI – Ostensible Intergalactic Cyber Electronic Portal – Military and Cyber Commands

https://easytech4all.net/2024/03/04/cyber-ai-ostensible-intergalactic-cyber-electronic-portal-military-and-cyber-commands/

Watch on YouTube

https://youtu.be/tayADWGwVUE?si=xKsIm280KfHD1z8z

After-hours Conversations between binary digits 0 and 1 at the Cyber Intelligence Command Center of a Global Military Alliance HQ somewhere in the Northern Hemisphere (Textual Simulation)

https://1powercyber.substack.com/p/after-hours-conversations-between

https://easytech4all.net/2024/03/20/after-hours-conversations-between-binary-digits-0-and-1-at-the-cyber-intelligence-command-center-of-a-global-military-alliance-hq-somewhere-in-the-northern-hemisphere/

Random Simulation – Multidimensional and Conjectural – Military Govt and Emergency First Responders

https://easytech4all.net/2024/03/10/3929/

Global Cyber Electronic Defense Intelligence Resources -

https://app.simplenote.com/p/2cmvGG

Precognitive AI – Clairvoyant or Appurtenant Invention (or Discovery)

https://easytech4all.net/2023/12/21/precognitive-ai-clairvoyant-or-appurtenant-invention-or-discovery/

CyberAI-CyberAGI(Projection) – Global Military Intelligence Industrial Defense Complex.

https://easytech4all.net/2024/01/16/cyberai-cyberagiprojection-global-military-intelligence-industrial-defense-complex/

Article: Scientists just set a nuclear fusion record in a step toward unleashing the limitless, clean energy source

Scientists just set a nuclear fusion record in a step toward unleashing the limitless, clean energy source

https://www.cnn.com/2024/02/08/climate/nuclear-fusion-energy-milestone-climate/

A Conversation with the Founder of ChatGPT

https://youtu.be/cYklSPyE2dI?si=Zqbzf2c5MhhGI7Ii

AI Security Document released by NSA and CISA - Generated by Google Gemini on 29Nov 2023

Sure, here is a summary of the salient features of the AI security document released by NSA, CISA, and US Agencies:
Guidance for Securing AI is a joint security advisory issued by the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and other US government agencies. The document provides guidance for organizations on how to secure their AI systems and mitigate the risks associated with AI.
The document outlines four key areas of AI system development:
Secure design: This includes identifying and addressing potential security vulnerabilities early in the design process.
Secure development: This includes using secure coding practices and implementing appropriate security controls throughout the development lifecycle.
Secure deployment: This includes deploying AI systems in a secure environment and monitoring for potential threats.
Secure operation: This includes maintaining and updating AI systems to address new threats and vulnerabilities.
The document also provides specific guidance on a number of security topics, including:
Data security: Protecting the confidentiality, integrity, and availability of data used to train and operate AI systems.
Model security: Ensuring that AI models are not vulnerable to manipulation or poisoning.
Privacy: Protecting the privacy of individuals whose data is used to train and operate AI systems.
Ethics: Ensuring that AI systems are used in a responsible and ethical manner.
The Guidance for Securing AI is a valuable resource for organizations that are developing or using AI systems. It provides a comprehensive overview of the security risks associated with AI and offers practical guidance on how to mitigate those risks.
Here are some additional salient features of the document:
It emphasizes the importance of a risk-based approach to AI security.
It recognizes that AI security is an ongoing process that requires continuous monitoring and improvement.
It encourages organizations to share information about AI security threats and vulnerabilities.
I hope this summary is helpful. Please let me know if you have any other questions.

Atos Digital Battle Management System

https://youtu.be/rTJwwUFoSQQ?si=g-LUzBcqwgjps7uP

Building the Connected Battlefield for the Tactical Edge

https://youtu.be/U7XqyXi-9pE?si=k_LhZqw-2yHcNukq

Deepfake Threats and Countermeasures

Artificial intelligence (AI) can play a crucial role in combating the spread and impact of deepfakes by employing various techniques to detect, prevent, and mitigate the harm caused by these manipulated media. Here are some specific ways in which AI can serve as a countermeasure against deepfakes:

1. Deepfake Detection:

AI-powered deepfake detection tools can analyze audio, video, and text content to identify subtle anomalies and patterns that are indicative of manipulation. These tools employ machine learning algorithms trained on large datasets of real and fake media to learn the telltale signs of deepfakes, such as inconsistencies in facial expressions, skin texture, lighting, and audio synchronization.

2. Content Authentication:

AI-based content authentication techniques can embed digital fingerprints or watermarks into media content, creating a unique identifier that can be used to verify the authenticity of the content. These watermarks are designed to be resilient to manipulation and can be detected even if the content has been altered.

3. Media Provenance Verification:

AI algorithms can analyze the metadata and history of media content to track its origins and identify potential sources of manipulation. This can help to establish the authenticity of content and identify potential deepfakes that have been circulating online.

4. Social Media Monitoring:

AI-powered social media monitoring tools can scan social media platforms for potentially harmful deepfakes, identifying and flagging content that is likely to spread misinformation or cause harm. This can help to limit the reach of deepfakes and prevent them from causing widespread damage.

5. Public Awareness Campaigns:

AI-based tools can be used to create personalized and targeted public awareness campaigns that educate people about deepfakes and how to identify them. These campaigns can help to reduce the susceptibility of individuals to deepfake manipulation and promote critical thinking in the digital age.

In addition to these specific applications, AI can also contribute to the development of more sophisticated deepfake detection and prevention methods. As AI research continues to advance, we can expect to see even more innovative and effective ways to combat deepfakes and protect against their harmful effects.

Here's a list of some open-source (FOSS) tools to detect deepfakes:

1. **Deepstar:** Developed by ZeroFox, Deepstar is an open-source toolkit that provides a suite of tools for detecting, analyzing, and mitigating deepfakes. It includes a curated library of deepfake and real videos, a plug-in framework for testing and comparing different detection algorithms, and code for aiding in the creation of deepfake datasets.

2. **FakeFinder:** Created by IQT Labs, FakeFinder is an open-source framework that utilizes a combination of deep learning models and traditional image processing techniques to detect deepfakes. It aims to provide a comprehensive and robust solution for identifying manipulated media.

3. **DeepSafe:** Developed by Siddharth Sah, DeepSafe is an open-source deepfake detection platform that aggregates various detection models and provides a dashboard for visualizing and analyzing results. It also facilitates the creation of a dataset of potentially harmful deepfakes for further research and improvement of detection methods.

4. **Visual DeepFake Detection:** This open-source tool takes a different approach to deepfake detection, focusing on identifying anomalies in facial expressions, eye movements, and skin texture. It utilizes a combination of traditional image analysis techniques and machine learning to detect subtle signs of manipulation.

5. **FALdetector:** This open-source tool in Python is designed to detect Photoshopped faces by analyzing image metadata and identifying inconsistencies in lighting, shadows, and color patterns. It primarily focuses on detecting manipulations in still images

rather than videos.

6. **Deepware Scanner:** Developed by Deepware, Deepware Scanner is an open-source forensic tool that analyzes videos for signs of deepfaking. It employs a deep learning model trained on a large dataset of real and fake videos to identify anomalies and inconsistencies.

7. **Reality Defender:** Developed by Sensity, Reality Defender is an open-source deepfake detection tool that utilizes a combination of machine learning and image processing techniques to identify manipulated media. It is designed to be easily integrated into existing applications and workflows.

8. **DFV:** Developed by the University of California, Berkeley, DFV is an open-source deepfake detection framework that utilizes a combination of spatial and temporal features to identify manipulated videos. It is designed to be lightweight and efficient, making it suitable for real-time applications.

9. **DeepFake-o-Meter:** This open-source tool provides a web-based interface for detecting deepfakes. It utilizes a combination of machine learning algorithms to analyze videos and provide a probability score indicating the likelihood of manipulation.

10. **Open Video Prediction Model (OVPM):** Developed by Facebook AI Research, OVPM is an open-source deep learning model for detecting deepfakes. It is trained on a large dataset of real and fake videos and can be used to identify manipulated videos with high accuracy.

These open-source tools represent a growing effort to combat the spread of deepfakes and protect against their harmful effects. As research continues to advance, we can expect to see even more sophisticated and effective FOSS tools emerge in the future.

https://www.linkedin.com/posts/danish-khan-easytech4all_deepfake-media-artificialintelligence-activity-6771673460205776896-1doe

NATO's Approach to Countering Disinformation

https://www.nato.int/cps/en/natohq/topics_219728.htm?selectedLocale=en

US Department of Defense Approach - Deepfake Disinfo Countermeasures

https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI-DEEPFAKE-THREATS.PDF&ved=2ahUKEwiUlpPy0K-CAxUn1zgGHVCfAVU4ChAWegQIExAB&usg=AOvVaw3uGBsI76VY0SAd0nJDcynU

German Government's approach to countering disinformation and Deepfakes

https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

https://www.scirp.org/journal/paperinformation.aspx?paperid=112520

https://www.semanticscholar.org/paper/DEEPFAKES%3A-THREATS-AND-COUNTERMEASURES-SYSTEMATIC-Albahar-Almalki/cd1cbbe9b7e5cb47c9f3aaf1b475d4694d9b2492

https://link.springer.com/article/10.1007/s10489-022-03766-z

https://www.socialproofsecurity.com/

Meet Rachel Tobac - Highly Proficient in Countering Social Engineering and Disinformation.

https://twitter.com/RachelTobac/status/1365413178327277575?s=19

Download Countersocial

CounterSocial - A Next-Gen Social Network

A unique social network. No trolls. No abuse. No ads. No fake-news. No foreign influence operations.

CounterSocial is the first Social Network Platform to take a zero-tolerance stance to hostile nations, bot accounts, trolls and disinformation networks who are weaponizing OUR own social media platforms and freedoms to engage in influence operations against us.

And we're here to counter it.

CounterSocial is 100% crowd powered by it's users, and does not run ads or 'promoted content'. Our users data is not mined or sold for any purpose.

https://play.google.com/store/apps/details?id=counter.social.android

Android Police: Android Open Source Project (AOSP): Everything you need to know

https://www.androidpolice.com/android-open-source-project-guide/

Spotlight: Open-Source Intelligence | #MSC2024

https://www.youtube.com/live/EoDBhMESzCg?si=PGwJTCmkQmM2ed1L

UN News: General Assembly adopts landmark resolution on artificial intelligence

https://news.un.org/en/story/2024/03/1147831

https://news.un.org//en/story/2024/03/1147831

https://twitter.com/antonioguterres/status/1720138955524334062

UN NEWS App

https://play.google.com/store/apps/details?id=org.un.mobile.news

UN News App stories relevant to Artificial Intelligence

https://news.un.org/en/story/2023/11/1143147

https://news.un.org/en/story/2023/10/1142867

https://news.un.org/en/story/2023/10/1142527

https://news.un.org/en/story/2023/07/1138397

https://news.un.org/en/story/2023/06/1137562

https://news.un.org/en/story/2023/06/1137302

https://twitter.com/UN_SPExperts/status/1664554550735302661

https://news.un.org/en/story/2023/07/1138827

https://news.un.org/en/story/2023/06/1137302

https://news.un.org/en/audio/2024/01/1145157

https://news.un.org/en/story/2021/09/1099972

https://twitter.com/UNHumanRights/status/1438111266015432711

https://news.un.org/

Defend against cyber threats with AI solutions from Microsoft

https://www.microsoft.com/en-us/industry/blog/government/defense-and-intelligence/2024/03/07/defend-against-cyber-threats-with-ai-solutions-
from-microsoft/

Artificial intelligence and the Futures of Learning

https://www.unesco.org/en/digital-education/ai-future-learning

European Cyber Agora.

https://www.microsoft.com/en-eu/cyber-agora/register.aspx

CNET: Nvidia 2024 AI Event: Everything Revealed in 16 Minutes

https://www.youtube.com/watch?v=bMIRhOXAjYk

Neuralink's first brain-chip patient plays online chess

https://www.youtube.com/watch?v=4m-Up6rbJZI

Elon Musk's brain implant company offers an intriguing glimpse of an internet connecting human minds

https://theconversation.com/elon-musks-brain-implant-company-offers-an-intriguing-glimpse-of-an-internet-connecting-human-minds-225382

Quantum Computing Breakthrough: Scientists Develop New Photonic Approach That Works at Room Temperature

https://scitechdaily.com/quantum-computing-breakthrough-scientists-develop-new-photonic-approach-that-works-at-room-temperature/

Defense Innovation Unit awards three contracts for space logistics technologies

https://spacenews.com/defense-innovation-unit-awards-three-contracts-for-space-logistics-technologies/

AI Military Integration

https://www.lawfaremedia.org/article/new-tools-are-needed-to-address-the-risks-posed-by-ai-military-integration

Nvidia CEO says AI could pass human tests in five years

https://www.reuters.com/technology/nvidia-ceo-says-ai-could-pass-human-tests-five-years-2024-03-01/

AURORA AT ARGONNE NATIONAL LABORATORY IN LEMONT ON TRACK TO BE WORLD'S FASTEST SUPERCOMPUTER

https://abc7chicago-com.cdn.ampproject.org/c/s/abc7chicago.com/amp/argonne-national-laboratory-lemont-il-aurora-supercomputer-climate-forecasting/14496197/

GPAI meet adopts New Delhi AI declaration

by Shouvik Das and Gulveen Aulakh, livemint.com
December 13, 2023 11:13 AM

NEW DELHI : The Global Partnership on Artificial Intelligence (GPAI) Summit, a congregation of 29 member nations including the European Union, on Wednesday announced the adoption of the New Delhi Declaration, according to the Union minister of state for information technology (IT) Rajeev Chandrasekhar. The declaration agreed to collaboratively develop AI applications in healthcare and agriculture, as well as including the needs of the Global South in development of AI.

Further, the declaration also saw participating nations agree upon using the GPAI platform to create a global framework on AI trust and safety, and make AI solutions and benefits available for all. India also pitched to host a GPAI Global Governance Summit to finalize the proposed framework, in six months.

“29 countries of the GPAI have unanimously adopted the New Delhi Declaration, which promises to position GPAI at the front and center of shaping the future of AI in terms of both innovation and creating collaborative AI between the partner nations. Countries agreed to create applications of AI in healthcare, agriculture, and many other areas that concern all our countries and all of our people," Chandrasekhar said.

He further added that GPAI will “be an inclusive movement that will focus on including countries in the Global South, and make available benefits of AI and AI platforms and solutions to the world including the people of the Global South."

A copy of the 14-point declaration was seen by Mint.

Visiting delegations at GPAI included Jean-Noel Barrot, minister of digital affairs for France; Hiroshi Yoshida, vice-minister of internal affairs for Japan; and Viscount Jonathan Camrose, minister of AI and intellectual property for the UK.

Congratulating Japan on setting up a third ‘expert support centre’ for AI alongside such existing centres in Canada and France, Barrot said, “In the next few months under the Indian presidency of GPAI, we will be discussing how we can pool some of our expert resources with that of OECD in order to extend our reach and ability to come up with the best possible solutions for the governance and the deployment of AI for the good of our people."

Both Yoshida and Camrose stressed upon the need for inclusivity as a key part of GPAI’s role in the global development of AI. Yoshida added that the body wants to “encourage more developing countries to join GPAI."

Following the conclusion of the GPAI Summit on Thursday, the Centre will unveil its official AI policy under the India AI Program on 10 January. Global discussions on the development of AI regulations will further take place at the Korea Safety Summit in mid-2024.

Earlier on Wednesday, in an interview with Mint, Chandrasekhar said that India's approach towards regulating AI comes as an intersection of enabling innovation, while enforcing guardrails that put checks on AI harm—a concern that India has raised before at November's UK AI Safety Summit.

"Governments have lagged innovation, and allowed it to go unregulated for many years. As a result, we have big islands of commercial power who are distorting the open nature of the internet, i.e; the Big Tech firms. This time, governments do not want to play catch up like before. The issue today is that regulating anything on the internet cannot happen in silos, because nearly 88% of harm sees perpetrators to be based in one jurisdiction, victims in a second jurisdiction, and the crime itself happening in a third one. Unless there is a global understanding in all of this, there's no point in India having a great regulation in AI harm if other nations do not," Chandrasekhar told Mint.

The minister further added that there is precedent on global regulatory agreements when it comes to addressing concerns of mass harm, such as in missile control or access to nuclear materials.

"There are global restrictions on how harmful technologies can be distributed, which we've seen in the past. AI can be as radioactive, if we allow it to be used by bad actors. That's the incentive for nations to realize the good, and recognize that people with access to it can also do really bad things. Therefore, no one country can play cop in cyberspace. Hence, we need a global legal framework," he said.

On Tuesday, prime minister Narendra Modi said that development of AI globally will use "humanitarian and democratic values."

"AI will have to be made all-inclusive and it will have to imbibe all ideas. The more its journey is inclusive, the better the results. Direction of AI development will depend on human and democratic values. It is up to us to keep a place for emotions along with efficiency, ethics and effectiveness," Modi said.

https://www.livemint.com/news/india/gpai-meet-adopts-new-delhi-ai-declaration-11702487342900.html

GPAI summit: Countries back India's approach on safe AI

by FE Bureau, financialexpress.com
December 13, 2023 10:57 PM

Twenty-nine-member countries, including India, the UK, Japan and France, which are part of the Global Partnership on Artificial Intelligence (GPAI), on Wednesday affirmed their commitment to work towards advanced, safe, secure, and trustworthy artificial intelligence (AI), while also looking at relevant regulations, policies, standards, and other initiatives. This assumes significance given that India, which is hosting the GPAI summit this year, and also the lead chair for GPAI in 2024, has been pitching for regulating AI through the prism of user harm, while not hindering the innovation.Further, all the member-countries have also agreed to jointly come up with a global set of basic principles that will shape the path for AI regulations."The 29-member countries have unanimously adopted the New Delhi declaration which promises to position GPAI at the front and the centre of shaping the future of AI in terms of both innovation and creating collaborative AI between partner nations," said Rajeev Chandrasekhar, minister of state for electronics and IT, on Day 2 of the GPAI summit in New Delhi."There is a serious consensus that we have to move fast as countries in broadly two directions. One is about deploying AI, collaborating work with like-minded countries in exploiting AI for healthcare, agriculture, sustainability, language translation, etc. At the same time, the countries are concerned with safety and trust issues that emerge from AI," Chandrasekhar added.Over the next few months, the countries will work together to lay out some broad principles on AI, including what guardrails should be there."We recognise the rapid pace of improvement in advanced AI systems and their potential to generate economic growth, innovation, and jobs across various sectors as well as to benefit societies. We acknowledge the need to harness new opportunities and mitigate the risks arising from the development, deployment, and use of such technologies," the declaration document of the GPAI ministers said.They also acknowledged the need for equitable access to resources, to be considered, accounted for, or addressed in order for societies to benefit from and build competitive AI solutions. "We underscore GPAI's pivotal role in addressing contemporary AI issues, including generative AI, through applied AI projects aimed at addressing societal problems and global challenges, maximising the benefits and mitigating associated risks," the document said.The member countries also agreed to India's pitch on developing the use of AI innovation in supporting sustainable agriculture as a new thematic priority for GPAI.

The ministers collectively agreed that a risk-proportionate trustworthy AI applications for ensuring sustainable food production systems and implementing resilient agricultural practices that increase productivity and production, help regenerate ecosystems, is crucial.

GPAI is an international initiative to support responsible and human-centric development and use of AI.

https://www.financialexpress.com/business/digital-transformation-gpai-summit-countries-back-indias-approach-on-safe-ai-3338294/

Internet Lookup –

“The UK Bletchley Declaration on AI”
“US President Executive Order – Data and AI Strategy”
“The US Department of Defense AI Adoption Strategy”

https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/

https://www.cisa.gov/ai

https://www.nato.int/cps/en/natohq/topics_219728.htm?selectedLocale=en

Precognitive AI in Futurism: Hype vs. Reality (Generated by Google Gemini)

The application of precognitive AI in future projections, threat modeling, and threat perception still remains largely **theoretical and experimental**. While the concept holds immense potential, significant challenges and ethical considerations hinder its widespread adoption in real-world scenarios.

Here’s a breakdown of the current landscape:

Hype and Potential:

1)GIDE experiments: Google’s internal “Global Information Diffusion Experiment” explored using AI to predict the spread of online misinformation, demonstrating a glimpse into AI’s potential for anticipating future events. AND THE OTHER G.I.D.E

Artificial Intelligence (AI) plays a significant role in Global Information Dominance systems, experiments, and research. Here are some ways AI has been utilized:

Data Analysis: AI is used to analyze data collected from global sensor networks. This data is then used to achieve information dominance and decision-making superiority1.

Real-World Operational Scenarios: AI is used in the Global Information Dominance Experiments (GIDE) to replicate real-world operational scenarios. This allows the U.S. Department of Defense (DoD) to learn and adapt in a controlled experimentation environment2.

Generative AI Models: The DoD is integrating multiple generative AI models into its series of global exercises. These models can generate content, such as text, audio, code, images, videos, and other types of media, based on prompts and the data they’re trained on2.

Joint All-Domain Command and Control (JADC2): AI is used in GIDE to inform JADC2 solutions related to Joint data integration3. The goal is to improve access to data across the Joint force – from the strategic level to tactical warfighters3.

Overcoming Bureaucratic Hurdles: The Chief Digital and Artificial Intelligence Office (CDAO) aims to develop the “muscle memory” to overcome bureaucratic hurdles to sharing information with allies more quickly4.

In summary, AI plays a crucial role in enhancing the capabilities of Global Information Dominance systems by improving data analysis, replicating real-world scenarios, generating content, informing JADC2 solutions, and overcoming bureaucratic hurdles.

2)Anomaly detection and pattern recognition: AI algorithms excel at identifying unusual patterns and deviations from established norms, which could be useful for flagging potential threats or emerging trends.

3)Scenario planning and simulation:Advanced AI models can simulate complex scenarios and analyze potential outcomes, aiding in proactive threat modeling and preparedness.

Challenges and Limitations:

Data quality and bias: AI predictions heavily rely on the quality and completeness of the training data. Biases within the data can lead to skewed or inaccurate predictions.

Black box problem: Complex AI models often lack transparency, making it difficult to understand the reasoning behind their predictions, hindering trust and accountability.

Ethical considerations:Precognitive AI raises ethical concerns around privacy, manipulation, and misuse of predictive power.

Current State of the Field:

* Primarily confined to research labs and pilot projects.

* Limited real-world applications due to the aforementioned challenges.

* Ongoing research and development efforts aim to address limitations and improve AI reliability and explainability.

Sources:

* “The Myth of Precognitive AI” by The Gradient (Google AI): https://cloud.google.com/blog/transform/prompt-debunking-five-generative-ai-misconceptions

* “Can AI Predict the Future?” by MIT Technology Review: https://medium.com/geekculture/magic-algorithms-does-ai-really-predict-the-future-9fe65c974ecc

* “GIDE: Global Information Diffusion Experiment” by Google Research: https://maps.google.com/localguides/

**Overall, while the potential of precognitive AI in futurism is significant, significant hurdles remain for homo sapiens to discover how it can be widely implemented in real-world applications cum scenarios . Responsible development and ethical considerations from a regulatory perspective will navigate this promising yet complex field.

Modern AI’s Dual Role in Cybersecurity: Offense and Defense

Simulating Cyber Attacks:

* **Red teaming:** AI can act as a sophisticated adversary, launching simulated cyber attacks to identify vulnerabilities in networks and systems. This proactive approach helps organizations patch weak spots before real attackers exploit them.

* **Stress testing:** AI can generate massive volumes of attack traffic, putting security infrastructure under immense pressure to reveal bottlenecks and potential points of failure. This stress testing ensures defenses can withstand real-world cyber assaults.

* **Evolving threats:** AI can continuously adapt its attack methods, mimicking the ever-changing tactics of real-world hackers. This keeps defenders on their toes and ensures their defenses stay relevant against the latest threats.

Sources:

* **Red Teaming with Artificial Intelligence:** https://www.ibm.com/x-force/team

* **Stress Testing Your Security with AI-Powered Attack Simulation:** https://www.paloaltonetworks.com/resources/datasheets/unit-42-incident-simulation-and-testing-services

* **The Future of Cyberwarfare: How AI is Changing the Game:** https://zapuza.com/technology/the-future-of-cybersecurity-how-ai-is-changing-the-game/

Cybersecurity Prevention:

* **Anomaly detection:** AI can analyze network traffic, system logs, and user behavior to identify anomalies that might indicate a cyber attack in progress. Early detection enables defenders to take swift action and mitigate potential damage.

* **Threat intelligence:** AI can process vast amounts of data from various sources to identify emerging cyber threats and vulnerabilities. This intelligence empowers defenders to stay ahead of attackers and proactively address potential risks.

* **Automated response:** AI-powered systems can automatically trigger countermeasures upon detecting a cyber attack, such as isolating infected systems or blocking malicious traffic. This rapid response minimizes the attack’s impact and buys time for human defenders to intervene.

Sources:

* **AI-Powered Anomaly Detection for Cybersecurity:** https://m.youtube.com/watch?v=1OSCF-pNwQk

* **The Power of AI in Threat Intelligence:** https://darktrace.com/

* **Automated Security Response: The Future of Cybersecurity:** https://www.paloaltonetworks.com/cortex/security-operations-automation

The Value of AI in the Military Metaverse:

* **Enhanced situational awareness:** AI can analyze vast amounts of data from sensors and simulations within the metaverse, providing commanders with a real-time, comprehensive picture of the battlefield. This enhanced awareness enables better decision-making and faster response times.

* **Improved training and simulations:** AI can create realistic and dynamic training scenarios within the metaverse, allowing soldiers to hone their skills and practice tactics in a safe, virtual environment. This improves combat readiness and preparedness.

* **Autonomous systems:** AI-powered drones, vehicles, and even weapons can operate within the metaverse, potentially reducing the need for human intervention in high-risk situations. This raises ethical concerns and necessitates careful development and deployment considerations.

Sources:

* **AI and the Military Metaverse:** https://www.cnas.org/research/technology-and-national-security/artificial-intelligence-ssp

* **The Rise of the Military Metaverse:** https://www.newyorker.com/humor/daily-shouts/life-in-the-fantastic-world-of-the-facebook-metaverse

* **The Ethics of AI in the Military Metaverse:** https://www.brookings.edu/articles/ai-makes-rules-for-the-metaverse-even-more-important/

Overall, AI plays a crucial role in both simulating and preventing cyber attacks, making our digital world safer. In the nascent Military Metaverse, AI holds immense potential for enhancing situational awareness, improving training, and even deploying autonomous systems. However, responsible development and ethical considerations are paramount to ensure AI's benefits outweigh the risks in this complex and evolving domain.

Remember, AI is a powerful tool, and its application in both offensive and defensive cybersecurity, as well as the military metaverse, requires careful consideration of its potential benefits and risks. As we navigate this new frontier, responsible development and ethical frameworks are essential to ensure AI serves humanity for the greater good.

I hope this information, along with the relevant images, provides a comprehensive understanding of AI's role in both offensive and defensive cybersecurity, as well as its potential value in the Military Metaverse. Please let me know if you have any further questions or want to explore specific aspects of this topic in more detail.

On SECOND REGENERATION – WITH SOME ADDITIVES

Modern AI's Dual Role in Cybersecurity: Offense and Defense

Simulating Cyber Attacks:

* **Red teaming:** AI can act as a sophisticated adversary, launching simulated cyber attacks to identify vulnerabilities in networks and systems. This proactive approach helps organizations patch weak spots before real attackers exploit them.

[Image of AI Red Team hacking a network]

* **Stress testing:** AI can generate massive volumes of attack traffic, putting security infrastructure under immense pressure to reveal bottlenecks and potential points of failure. This stress testing ensures defenses can withstand real-world cyber assaults.

[Image of AI stress testing a network]

* **Evolving threats:** AI can continuously adapt its attack methods, mimicking the ever-changing tactics of real-world hackers. This keeps defenders on their toes and ensures their defenses stay relevant against the latest threats.

[Image of AI evolving cyber attack methods]

Cybersecurity Prevention:

* **Anomaly detection:** AI can analyze network traffic, system logs, and user behavior to identify anomalies that might indicate a cyber attack in progress. Early detection enables defenders to take swift action and mitigate potential damage.

[Image of AI detecting anomalies in network traffic]

* **Threat intelligence:** AI can process vast amounts of data from various sources to identify emerging cyber threats and vulnerabilities. This intelligence empowers defenders to stay ahead of attackers and proactively address potential risks.

[Image of AI processing threat intelligence data]

* **Automated response:** AI-powered systems can automatically trigger countermeasures upon detecting a cyber attack, such as isolating infected systems or blocking malicious traffic. This rapid response minimizes the attack's impact and buys time for human defenders to intervene.

[Image of AI automatically responding to a cyber attack]

The Value of AI in the Military Metaverse:

* **Enhanced situational awareness:** AI can analyze vast amounts of data from sensors and simulations within the metaverse, providing commanders with a real-time, comprehensive picture of the battlefield. This enhanced awareness enables better decision-making and faster response times.

* **Improved training and simulations:** AI can create realistic and dynamic training scenarios within the metaverse, allowing soldiers to hone their skills and practice tactics in a safe, virtual environment. This improves combat readiness and preparedness.

[Image of AI-powered training simulations in the metaverse]

* **Autonomous systems:** AI-powered drones, vehicles, and even weapons can operate within the metaverse, potentially reducing the need for human intervention in high-risk situations. This raises ethical concerns and necessitates careful development and deployment considerations.

Overall, AI plays a crucial role in both simulating and preventing cyber attacks, making our digital world safer. In the nascent Military Metaverse, AI holds immense potential for enhancing situational awareness, improving training, and even deploying autonomous systems. However, responsible development and ethical considerations are paramount to ensure AI's benefits outweigh the risks in this complex and evolving domain.

Remember, AI is a powerful tool, and its application in both offensive and defensive cybersecurity, as well as the military metaverse, requires careful consideration of its potential benefits and risks. As we navigate this new frontier, responsible development and ethical frameworks are essential to ensure AI serves humanity for the greater good.

WEF and INTERPOL - Cybersecurity Global event

Resources and Links.

https://www.weforum.org/projects/cyber-polygon

https://cyberpolygon.com/

https://www.weforum.org/join-us/home

Watch the Recording.

https://cyberpolygon.com/gallery/

https://1powercyber.substack.com/p/wef-and-interpol-cybersecurity-mega?utm_source=pocket_mylist

UN Security Council Cyber Threats Debate

https://easytech4all.net/2022/03/06/un-security-council-cyberthreats-debate/

UNIDIR Cyber Stability Congerence

https://easytech4all.net/2022/07/05/unidir-cyber-stability-conference-3rd-december-friday-2021/

https://1powercyber.substack.com/p/wef-and-interpol-cybersecurity-mega/

http://easytech4all.net/2022/07/05/unidir-cyber-stability-conference-3rd-december-friday-2021/?utm_source=pocket_mylist

2022 Cyber Stability Conference: Protecting Critical Infrastructure and Services Across Sectors
unidir.org

https://unidir.org/CS22?utm_source=pocket_mylist

UNIDIR - Improving Space Security and sustainability

https://unidir.org/projects/improving-space-security-and-sustainability?utm_source=pocket_mylist

UNIDIR - AI and Weaponisation AWS

https://unidir.org/projects/artificial-intelligence-and-weaponization-increasingly-autonomous-technologies?utm_source=pocket_mylist

UNIDIR - Cyber Stability

https://unidir.org/projects/cyber-stability?utm_source=pocket_mylist

UNIDIR - Security Dimensions Innovations Science and Technology

https://unidir.org/projects/security-dimensions-innovations-science-and-technology?utm_source=pocket_mylist

UNIDIR - Cyber Nuclear Nexus

https://www.unidir.org/publication/cyber-nuclear-nexus-summary-nuclear-risk-reduction-workshop-series?utm_source=pocket_mylist

Mathematical calculations show that quantum communication across interstellar space should be possible

https://flip.it/wQfS9t?utm_source=pocket_mylist

Statement by President Biden on our Nation's Cybersecurity

https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/?utm_source=pocket_mylist

White House to boost support for quantum technology while boosting cybersecurity

https://www.reuters.com/world/us/white-house-boost-support-quantum-technology-while-boosting-cybersecurity-2022-05-04/?utm_source=pocket_mylist

Fourth Annual National Security Conference

Amidst intensifying globalization, sound security policies require the collaboration of multiple branches of government agencies and the military services, among others.

William & Mary's Whole of Government Center of Excellence (WGC) trains and educates a new generation of future leaders who have hands-on, practical experience working across the different organizational cultures. Through our strategic leader training certificates and programs, research collaborations and convenings, and W&M degree programs, the WGC cultivates acculturation. Based on a few hundred years of history, we find that interagency cultures should be taught, understood, and harmonized by the men and women tasked with working among and between agencies and units. With that knowledge base, our networks and students are equipped to navigate the twists, tunnels, and shortcuts during a national security emergency, strategy development and implementation, or foreign deployment whether they are a GS-5 or a Lieutenant Colonel.

About the Whole of Government Center of Excellence

The William & Mary Whole of Government Center of Excellence (WGC) provides mid-career public policy professionals and military officers in federal, state, and local agencies with practical training on interagency collaboration, complex national security, and other public policy problems. WGC brings together leaders from all levels of government and military for symposia, discussions, and projects to promote creative, collaborative research and solutions to emerging issues. Currently, WGC is developing a national security curriculum, including e-learning opportunities, and research partnerships while providing customized non-degree training and education certificates for a variety of partners. Unlike other national security programs, W&M invokes the "whole of university" approach to our education, training, and research programs, leveraging partnerships with W&M Law School, Business School, Virginia Institute of Marine Sciences, School of Education, and departments across the Arts & Sciences.

4th Annual National Security Conference
Friday | March 22 | 8:30 a.m. - 5:00 p.m. | Brinkley Commons | Mason School of Business

WMGIC NATO Collaborate for 4th Annual Disinformation Challenge

https://www.wm.edu/offices/wholeofgovernment/news/wmgic-and-nato-collaborate-for-4th-annual-global-disinformation-challenge.php

NATO CCDCOE WMGIC Cybersecurity Challenge ebook

https://www.wm.edu/offices/revescenter/news/2022/nato-ccdcoe-and-wmgic-release-cybersecurity-challenge-e-book.php

https://www.linkedin.com/company/william-mary-whole-of-government-center-of-excellence/

Join LiveStream

https://www.youtube.com/watch?v=FKxzWl33Mko

Join Mailing List

https://wmsas.qualtrics.com/jfe/form/SV_bQ81wye1W05TzBY

https://www.wm.edu/offices/wholeofgovernment/

https://www.youtube.com/live/FKxzWl33Mko?si=S-NtQkMa7mcI4eGt

https://youtube.com/@wgcwm?si=gUloVidxKqd1zyje

https://youtube.com/@wgcwm?si=2BZBCRUDdoClP2UP

https://www.wm.edu/offices/wholeofgovernment/

Speaker Agenda

All times are Eastern Daylight Time (EDT). Additional speakers will be added when confirmed.

Thurs. March 21

5:00 - 6:30 p.m. Fireside Chat: “Data Revolution and National Security Evolution”
Shane Harris, Intelligence and National Security Correspondent, The Washington Post

Stephanie Pell, Fellow in Governance Studies, Brookings Institution, and Senior Editor, Lawfare

Friday, March 22

8:30 - 8:45 a.m. Introduction & Welcome Remarks

Peggy Agouris, Provost, William & Mary
Kathryn H. Floyd, Director, Whole of Government Center of Excellence, William & Mary

8:45 - 9:45 a.m. Senior Leadership Panel: “Future of Data, AI, & Cyber Defense”

Senior leaders will provide a thought-provoking fireside chat that will delve into the dynamic landscape of data management, artificial intelligence, and cybersecurity, exploring their pivotal roles in shaping the future of national defense strategies. The discussion will include cutting-edge technologies, emerging threats, and innovative solutions poised to redefine how nations safeguard their interests in an increasingly digital world. Gain invaluable insights into the intersection of data analytics, AI-driven decision-making, and robust cyber defense measures, ensuring readiness and resilience in the face of evolving security challenges.

Panelists:

Chon Abraham, Mansfield Professor of Business/Information Systems, Raymond A. Mason School of Business, William & Mary

Lashon Booker, PhD, Senior Principal Scientist, Acting Chief Engineer, Artifical Intelligence & Autonomy Innovation Center

Piret Pernik, Cybersecurity Researcher, NATO Cooperative Cyber Defence Centre of Excellence

Eileen Vidrine, Chief Data and AI Officer, U.S. Air Force

9:45 - 10:45 a.m. Panel #1: “Compliance vs. Security vs. Privacy”

Distinguished experts will convene to dissect the complex challenges and opportunities inherent in reconciling regulatory compliance requirements, robust security protocols, and the imperative of safeguarding individual privacy rights. Through dynamic dialogue, attendees will gain a comprehensive understanding of the delicate balance required to navigate these critical domains effectively, offering invaluable insights for business, defense, and policymakers alike.

Panelists:

Rob Cochran, Co-founder, Bawn, former Cyber Crimes Investigations Supervisor, Federal Bureau of Investigation (ret.)

Andrea Matwyshyn, Professor of Law and Engineering Policy/Professor of Engineering Design, Penn State Law/Penn State Engineering

Przemek Praszczalek, Director, Identity Products & Innovation, Cybersecurity & Intelligence division, Mastercard Inc.

Anthony Stefanidis, Professor of Computer Science, Director, William & Mary Data Science
Edward Tuorinsky, Founder & Managing Principal, DTS

10:45 - 11:00 a.m. Networking Break

11:00 - 11:35 a.m. Keynote Address

Eric Goldstein, Executive Assistant Director for Cybersecurity (CSD), Cybersecurity and Infrastructure Security Agency (CISA)

11:35 a.m. - 1:00 p.m. Working Lunch
Presentations by Project on International Peace and Security fellows, William & Mary Global Innovation Challenge leaders, and more

1:00 - 2:00 p.m. Panel #2: Securing Critical Infrastructure in the Age of AI and other Emerging Technologies

Subject matter experts will dissect the evolving landscape of safeguarding essential infrastructure against emerging threats in an era defined by artificial intelligence and other emerging technologies. The panel will explore the intricate challenges and innovative
strategies aimed at fortifying critical assets against cyber-attacks and disruptions. Join us for a dynamic exchange of insights and best practices, as we collectively navigate the intersection of AI, emerging technology, cybersecurity, and national defense in ensuring the resilience and integrity of vital infrastructure networks.

Panelists:

Glenn Ballard, President/CEO, Founder, Dragonfli Group

Dan Bowden, CISO, Marsh Global

David Burg, Americas Cyber Leader, EY

Iria Giuffrida, Assistant Dean for Academic & Faculty Affairs, Professor of the Practice of Law, William & Mary Law School

Tracy Gregorio, CEO, G2 Ops, Inc.

2:00 - 2:30 p.m. Special Address by Major General Ring, 29th Adjutant General of Virginia

2:30 - 2:45 p.m. Networking Break

2:45 - 3:45 p.m. Panel #3: Cyber Attacks, AI Weaponry, & the Future of National Security Policy

This panel will explore how cyber conflict and Artificial Intelligence (AI) and other emerging technologies are impacting national security strategies, and a transformation of military modernization and intelligence approaches. Contemporary threats, including information warfare and cyber attacks, require a reexamination of governance frameworks surrounding AI oversight, and strengthening cybersecurity and data privacy. The national security implications of AI, therefore, involves a close interrogation of the role of domestic and international law in regulating AI tools to mitigate a growing body of threats that are technologically-driven and rely upon AI weaponry.

Panelists:

Jocelyn Aqua, Principal of Data, risk, Privacy, & AI Governance, PricewaterhouseCoopers (PwC)

Merritt Baer, Merritt Baer, CISO; Advisor, Expanso; Board of Advisors, BlackGirlsHack; Co-Founder, Tech and Roses; former Deputy CISO, AWS

Ashley Deeks, Class of 1948 Professor of Scholarly Research in Law, University of Virginia Law School

Trenton Ford, Assistant Professor of Data Science, William & Mary

Margaret Hu, Taylor Reveley Research Professor, Professor of Law, William & Mary Law School

Davi Ottenheimer, Vice President of Trust and Digital Ethics, Inrupt

Russ Travers, Senior Advisor, DHS Office of Intelligence and Analysis, former Acting Director and Deputy Director, National Counterterrorism Center

3:45 - 4:45 p.m. Panel #4: Understanding the New Landscape for Security
In an information society and digital economy, it is increasingly imperative to consider how best to balance technological innovation aims with democratic and constitutional governance objectives. Vision 2026, W&M's strategic plan, invites a conversation on data and democracy. This interdisciplinary panel led by the Global Research Institute (GRI) explores how national

security goals are inclusive of broader conceptualizations of security, including cognitive security, climate and water/environmental preservation, health and food security, and data protection and cybersecurity. This panel discusses how the new landscape for security has the potential to reinforce democracy.

Panelists:

Kira Allmann, Ph.D., Director, Partnerships & Communications, Global Research Institute, William & Mary

Amy Gaudion, Associate Professor of Law, Penn State Dickinson Law, and Founder of Annual Cyberspace

Simulation with U.S. Army War College
Elizabeth Losh, Ph.D., Duane A. and Virginia S. Dittman Professor of English & American Studies

Julia Mossbridge, Research Director, Mossbridge Institute; Founder, TILT: The Institute for Love and Time;

Affiliated Professor, University of San Diego Dept of Physics and Biophysics
Roger Yee, Managing Partner, Outcome/One

4:45 p.m. Closing Remarks

Android Police: Android Open Source Project (AOSP): Everything you need to know

https://www.androidpolice.com/android-open-source-project-guide/

Spotlight: Open-Source Intelligence | #MSC2024

https://www.youtube.com/live/EoDBhMESzCg?si=PGwJTCmkQmM2ed1L